الجرائم المعلوماتية الواقعة عبر مواقع التواصل الاجتماعي
قراءة في قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 ونظام مكافحة جرائم المعلوماتية السعودي 1428هـ.

د. أحمد حسن عبد العليم حسن الخطيب

كلية العلوم والآداب جامعة شقراء، المملكة العربية السعودية

الملخص :تعد الجرائم المعلوماتية من الجرائم الحديثة نسبياً، فهي ظاهرة إجرامية جديدة تدق ناقوس الخطر لكافة الدول لتنبهها من المخاطر التي تنجم عنها، حيث تهدف الجرائم المعلوماتية الى الاعتداء على كافة البرامج المخزنة داخل الحاسب الآلي أو الموجودة على شبكة "الإنترنت"، وتكمن خطورة تلك الجرائم في كونها تنشأ وتعد وتتطور سراً، يقوم عليها مجموعة من المجرمين الذين يتمتعون بدرجة عالية من الذكاء، ولهم مهارة فائقة في استخدام وسائل التكنولوجيا، وأهم ما يميز هؤلاء امتلاكهم قدر كبير من أدوات المعرفة التكنولوجية.

ونظراً لخطورة هذا النوع من الجرائم نتناول في التمهيد عن بيان ماهية شبكات التواصل الاجتماعي والجرائم المعلوماتية، بينما نتناول في المبحث الاول بيان أهم الجرائم المرتكبة عبر المواقع الإلكترونية، وفي المبحث الثاني نلقي الضوء على دور المواقع الالكترونية في عملية جمع الاستدلالات، وأخيرا نتناول في المبحث الثالث بيان موقف كلاً من المشرع المصري والمنظم السعودي تجاه جرائم تقنية المعلومات.

<u>**The summary:**</u> The IT crimes are considered one of the modern crimes nowadays. It is a new criminal phenomenon which warns many countries and threatens them from the riskiness which happens because of it. The IT crimes aim to penetrate all the stored programs in the computer or which exist on the Web. The dangerousness of these crimes is that they are emerged, edited and developed in a secret way. The criminals of these crimes are extremely intelligent and have a great skill in using means of technology. The most important qualification of those people is that they have enormous amount of technical knowledge.

According to the riskiness of that kind of crimes, we talk in the introduction about the nature of the social communication networks and the IT crimes. In the first research, we clarify the most important crimes which are committed through the websites. In the second research, we highlight the role of the websites in the operation of collecting inferences. Finally, we show in the third research the situation of the Egyptian legislator and the Saudi regulator towards the IT crimes.

المقدمة:

تعد المواقع الالكترونية ومواقع التواصـــــل الاجتماعي هي شـــبكات الكترونية تهدف إلي تحقيق التواصل الاجتماعي بين الأشخاص في مختلف بقاع العالم، فهي شبكات تحقق تواصل اجتماعي بشكل افتراضـي بين الأشـخاص، وإذا كانت تلك الشبكات تحقق التواصل الاجتماعي بشكل أسرع، فضـلاً عن كونها تعمل على توفير الجهد والوقت والمال في جمع المعلومات، وكونها وبحق تقرب التواصـــــل بين الناس بشكل اكثر من رائع، إلا أن هناك من يستخدمها بشكل سيء للغاية ويرتكب من خلالها الكثير من الجرائم ظناً منه أنه بمنأى عن المحاسبة، أن يد العدالة لا يمكن أن تطاله، فشبكات التواصل الاجتماعي ســـهلت بشـــكل كبير ارتكاب الكثير من الجرائم ، حيث أنه يمكن من خلالها التوصـــل إلى جميع أنواع المعلومات الشـخصية الخاصة بالأفراد وهوايتهم، كما ان هناك كم رهيب من الإعلانات المنتشرة عبر تلك الشبكات والتي تكون في معظمها إعلانات وهمية مخالفة في الغالب الأعم لحقيقتها مما يدخل تدليس على الأفراد.

وعلى الرغم من مساوئ المواقع الالكترونية ومواقع التواصل الاجتماعي نظراً لكونها مرتعاً خصباً لارتكاب تلك الجرائم إلا أنها تمثل في ذات الوقت فرصـــة حقيقية للشـــرطة في جمع الاســـتدلالات عن الجرائم التي تقع بواســـطتها، فمن خلال تحليل محتوى الشـــبكات يمكن تحديد العلاقة بين المشـــتبه فيهم، والجرائم الناشـئة عن اسـتخدام شـبكات التواصـل الاجتماعي ، حيث تلعب هذه المواقع في زيادة ارتكاب الجرائم.

أهمية البحث:

تبرز أهمية البحث في كونه يتناول الحديث عن جرائم التواصل الاجتماعي حيث يوضح أهم الجرائم التي ترتكب بواسطة استخدام مواقع التواصل الاجتماعي، مع بيان الدور الذي تلعبه هذه المواقع في جمع الاستدلالات والمعلومات علي المجرم، كما تبرز أهمية هذا البحث في كونه يوضح دور المشرع المصري في مثل هذه الجرائم وآليات التصدي لها.

أهداف البحث:

تهدف هذا البحث الي البحث في موضوع جرائم التواصل الاجتماعي، خصوصاً وأن المشرع يولي اهتماماً كبيراً لمثل هذه الجرائم وذلك لخطورتها علي المجتمع وصعوبة الامساك بها، كما يهدف البحث الي بيان الآتي:

- ✓ الجرائم التي ترتكب علي مواقع التواصل الاجتماعي.
- ✓ الدور الذي تلعبه مواقع التواصل الاجتماعي في جمع الاستدلالات.
- ✓ موقف المشـــرع المصـــري في قانون مكافحة جرائم تقنية المعلومات المصـــري رقم 175 لسنة 2018 تجاه الجرائم المرتبكة عبر مواقع التواصل الاجتماعي والمواقع الالكترونية.

- ✓ موقف المنظم السـعودي في نظام مكافحة جرائم المعلوماتية 1428هـ تجاه الجرائم المرتكبة عبر مواقع التواصل الاجتماعي والمواقع الالكترونية.

مشكلة البحث:

تتمثل مشكلة البحث في سهولة ارتكاب الجرائم الالكترونية عبر مواقع التواصل الاجتماعي وولوج الأشخاص لتلك المواقع بأسماء وصفحات وهمية الأمر الذي يصعب معه الامساك بمرتكبي تلك الجرائم، كما تبرز مشكلة البحث في كونه يحاول الاجابة علي سؤال رئيس يتمثل في **ما هي الجرائم التي ترتكب عبر مواقع التواصل الاجتماعي وكيف تصدي المشرع المصري والسعودي لمواجهة تلك الجرائم؟.**

ويطرح البحث مجموعة من الأسئلة يحاول الإجابة عنها وتتمثل هذه الأسئلة في الآتي:

- ✓ ما هي أهم الجرائم المرتكبة عبر مواقع التواصل الاجتماعي؟.
- ✓ ما هو الدور الذي تلعبه مواقع التواصل الاجتماعي في جمع الاستدلالات؟.
- ✓ ما هي أهم الملامح التي اتخذها المشـرع المصـري في قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 تجاه الجرائم المرتبكة عبر مواقع التواصل الاجتماعي؟.
- ✓ ما هي أهم الملامح التي اتخذها المنظم السـعودي في نظام مكافحة جرائم المعلوماتية 1428 هـ تجاه الجرائم المرتبكة عبر مواقع التواصل الاجتماعي؟.

منهجية البحث:

يتبع الباحث المنهج التحليلي في بحثه للجرائم الواقعة عبر مواقع التواصـل الاجتماعي؛ حيث يعمل على استقراء نصوص قانون مكافحة قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018، ونظام جرائم المعلوماتية السعودي 1428هـ، وبيان أهم الملامح التي اتخذها المشـرع المصـري والمنظم السعودي في قانون مكافحة جرائم تقنية المعلومات.

خطة البحث:

المقدمة:

تمهيد: ماهية شبكات التواصل الاجتماعي والجرائم المعلوماتية.

المبحث الاول: أهم الجرائم المرتكبة عبر المواقع الإلكترونية.

المبحث الثاني: دور المواقع الالكترونية في عملية جمع الاستدلالات.

المبحث الثالث: موقف المشرع المصري والسعودي تجاه جرائم تقنية المعلومات.

الخاتمة.

النتائج والتوصيات.

قائمة المراجع.

تمهيد: ماهية شبكات التواصل الاجتماعي والجريمة المعلوماتية:

أولاً: ماهية شبكات التواصل الاجتماعي:

شبكة التواصل الاجتماعية هي وسيلة الكترونية حديثة للتواصل الاجتماعي، حيث إنها تكون بنية اجتماعية افتراضية تجمع بين أشخاص أو منظمات تتمثل في نقاط التقاء متصلة بنوع محدد من الروابط الاجتماعية؛ إذ يجمع المشاركين فيها صداقة أو قرابة أو مصالح مشتركة، أو توافق في الهواية أو الفكر، أو رغبة في التبادل المادي أو المعرفي، أو محبة أو كراهية لشيء معين، أو علاقات عقدية أو دينية، أو تناسق في المعرفة أو المركز الاجتماعي.

فإذا كانت شبكات التواصل الاجتماعي توفر الجهد والوقت والمال في جمع المعلومات، فمن خلالها يمكن ارتكاب الكثير من الجرائم، كما يمكن من خلالها أيضاً التوصل إلى جميع أنواع المعلومات الشخصية الخاصة بالفرد أيضاً، وهذا يمثل فرصة حقيقية للشرطة في جمع الاستدلالات عن الجرائم التي تقع عليها، فمن خلال تحليل محتوى الشبكات يمكن تحديد العلاقة بين المشتبه فيهم، والجرائم الناشئة عن استخدام شبكات التواصل الاجتماعي، حيث تلعب هذه المواقع في زيادة ارتكاب الجرائم.

ونري أنه ونتيجة لانتشار مواقع التواصل الاجتماعي أصبح الإنسان يعاني في سبيل الحفاظ علي خصوصيته الشخصية التي أصبحت هدفاً لبعض مستخدمي تقنية التواصل الاجتماعي بحسن نية أو بضدها، وذلك نظراً لأن مستخدمي شبكات التواصل الاجتماعي يضعون الكثير من خصوصياتهم في هذه المواقع، فإن انتهاكها والتطفل عليها باستخدام شتي الوسائل في الوصول إلي هذه الخصوصية أصبح مشكلة تؤرق مستخدمي هذه المواقع وأثر ذلك سلباً عليه سواء مادياً أو معنوياً، كما تبرز اشكالية البحث في صعوبة الامساك بمرتكبي الجرائم التي تقع عبر الانترنت عموماً ومواقع التواصل الاجتماعي خصوصاً.

فشبكات التواصل الاجتماعي هي منظومة الكترونية تتم صناعتها من قبل أفراد أو جماعات أو مؤسسات قائمة على مجموعة من العلاقات، هذه العلاقات قد تصل لدرجات اكثر عمقاً كطبيعة الوضع الاجتماعي أو المعتقدات أو الطبقة التي ينتمي إليها الشخص، فهي شبكة مواقع فعالة جداً في تسهيل

الحياة الاجتماعية بين مجموعة من المعارف والاصـــدقاء، كما تمكن الأصـــدقاء القدامى من التواصـــل المرئي والصوتي وغيرها من الامكانات التي توطد العلاقة الاجتماعية فيما بينهم [130].

ويمكن لنا تعريف وســـائل التواصـــل الاجتماعي بأنها: (**تلك الوســـائل التقنية الحديثة التي يســتخدمها الأشــخاص فيما بينهم لتحقيق التواصـل الاجتماعي المشـاع عبر شـبكة الانترنت كالفيس بوك، تويتر، اليوتيوب، وغيرها من مواقع التواصل الاجتماعي)** .

ثانياً: ماهية الجريمة المعلوماتية:

تعد الجرائم المعلوماتية من الجرائم الحديثة، فهي ظاهرة إجرامية جديدة تدق ناقوس الخطر لكافة الدول والجماعات لتنبهها من المخاطر التي تنجم عنها، وتحذرها من هول الخســـائر الناجمة عنها، فهي تعتدي على المعطيات بدلالتها التقنية الواســـعة، وتخترق المعلومات والبيانات, وتدخل الى البرامج بكافة أنواعها, كما تهدف هذه الجرائم الى الاعتداء على كافة البرامج المخزنة داخل الحاســـب الآلي أو تلك البرامج المنقولة عبر الشـــبكة العنكبوتية "الإنترنت"، كما تعتبر هذه الجريمة من الجرائم التي تعتم على التقنية المعلوماتية، وتكمن خطورتها في كونها تنشأ وتعد وتتطور سراً، يقوم عليها مجموعة من المجرمين الذين يتمتعون بدرجة عالية من الذكاء، ولهم مهارة فائقة في اســتخدام وســائل التكنولوجيا، وأهم ما يميز هؤلاء امتلاكهم قدر كبير من أدوات المعرفة التكنولوجية.

ويقصـــد بالجريمة المعلوماتية في النظام الســـعودي بأنها: (أي فعل يرتكب متضـــمناً اســـتخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام) [131].

ويمكن تعريف الجريمة المعلوماتية هي: (كل ســلوك ســلبي أو إيجابي يتم بموجبه الاعتداء على البرامج أو المعلومات أو الاستفادة منها بأية صورة كانت) [132].

المبحث الاول

أهم الجرائم المرتكبة عبر المواقع الالكترونية

تمهيد وتقسيم :

130. د. رانيا عبد الله الشريف، دور وسائل التواصل الاجتماعي في انتشار الشائعات، بحث مقدم لمجلة العلاقات العامة والإعلان، الجمعية السعودية للعلاقات العامة والإعلان، السعودية، العدد 3، 2015م، ص 89 .

131. المادة الأولي الفقرة الثامنة من نظام مكافحة جرائم المعلوماتية 1428هـ، مرسوم ملكي رقم: م/17 بتاريخ 1428/3/8هـ.

132. د. محمد محمد سيد احمد عامر، المسؤولية الجنائية عن ترويج الإشاعات عبر وسائل التواصل الاجتماعي دراسة فقهية مقارنة بالقانون المصري والنظام السعودي، بحث مقدم لمؤتمر وسائل التواصل الاجتماعي التطبيقات والإشكاليات المنهجية ، كلية الإعلام والاتصال، جامعة الإمام محمد بن سعود الإسلامية، الرياض، الفترة من19-1436/5/20هـ الموافق 10-2015/3/11م ، ص 6 .

صاحب ظهور شبكة الانترنت وشبكات التواصل الاجتماعي والمواقع الالكترونية تطورات كبيرة في شتي المجالات، وظهرت الكثير من الجرائم المستحدثة التي تستهدف الكثير من القطاعات، مما جعل من مأمورية الفقهاء فيما يخص تحديدها وتصنيفها يتميز بالصعوبة، علي عكس الجرائم التقليدية التي يمكن تصنيفها بسهولة فائقة.

أولا: جرائم سرقة الهوية والبيانات الشخصية.

يعرف المشرع المصري في قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018م البيانات الشخصية بأنها أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى[133].

كما يُقصد بسرقة الهوية الحصول بوسائل احتيالية على معلومات من الإنترنت تخص شخصاً معيناً، مثل (الاسم، وتاريخ الميلاد، والمهنة، والجنسية) دون علمه، ويقع ذلك في الأغلب الأعم بهدف ارتكاب جرائم احتيال إلكتروني، ومن ذلك أن ينتحل الجاني هوية شخص معين، ويحصل على قروض أو بطاقات ائتمان، أو يقوم بفتح حساب مصرفي، والاحتيال يتم باستخدام طرق احتيالية يوهم من أجلها المجني عليه بوجود مشروع كاذب أو يحدث أمل لديه بحصول ربح، فيسلم المال للجاني بطريق معلوماتي أو من خلال تصرف الجاني في المال وهو يعلم أن ليس له صفة التصرف فيه، وقد يتخذ اسم وصفة كاذبة تمكنه من الاستيلاء علي مال المجني عليه فيتم التحويل الالكتروني للأموال وذلك من خلال اتصال الجاني بالمجني عليه عن طريق الشبكة أو يتعامل الجاني مباشرة مع بيانات الحاسب فيستعمل البيانات الكاذبة التي تساعد في إيهام الحاسب والاحتيال عليه فيسلمه النظام المال [134].

ومع ذلك لوحظ في الآونة الأخيرة أن جرائم سرقة الهوية قد تُرتكب لا من أجل الربح، وإنما لأجل إيذاء شخص، أو بهدف الحصول على خدمة من أجل المتعة، حيث وتشير الإحصاءات إلى أن 10 ملايين شخص تعرضوا لسرقة الهوية في عام 2008، ومن التطبيقات على جرائم سرقة الهوية في الولايات المتحدة الأمريكية احتيال شخص على آخرين بادعائه أنه مالك لعقار بعد أن حصل على المعلومات الشخصية عن المالك الحقيقي من الإنترنت، واصطنع وثائق مزورة، وتمكن بذلك من بيع العقار لآخرين، وحصل منهم على مقابل مادي كبير، وفي فرنسا قُضي بتعويض امرأة عن الضرر الناجم عن قيام شخص بانتحال هويتها، وقام بوضع رقم هاتفها على مواقع اجتماعية، مدعياً أنها تمارس الدعارة، وحصل على

133. المادة الأولي من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.

134. د. خالد ممدوح ابراهيم ، امن الجريمة الالكترونية ، الدار الجامعية ، الاسكندرية ، 2010 م ، ص 76 .

أموال جراء ذلك، وبذلك يتضح أن سرقة الهوية تشكل خطورة على حقوق الأشخاص في الحفاظ على بياناتهم الشخصية [135] .

كما قد يتم انتحال الهوية مما يعمد اليه المجرم من استخدام هوية شخص اخر للاستفادة من سمعته مثلاً أو ماله أو صلاحياته، ولذلك فهذا سبب وجيه يدعوا للاهتمام بخصوصية وسرية المعلومات الشخصية للمستفيدين علي شبكة الانترنت، وتتخذ جريمة انتحال الهوية عبر الانترنت أحد الوجهيين التاليين: انتحال هوية الفرد، والثانية انتحال هوية المواقع، ولقد سماها بعض المختصين في أمن المعلومات جريمة الالفية الجديدة، وذلك نظراً لسرعة انتشار ارتكابها خاصة في الأوساط التجارية [136].

وتجدر الإشارة إلى أن كلاً من المشرع المصري والمنظم السعودي لما يضعا نصاً صريحاً يُجرم سرقة الهوية، وبالتالي لا تُعد جريمة سرقة الهوية في حد ذاتها جريمة، إلا إذا استتبعها سرقة وانتحال الشخصية، غير أن المشرع المصري أوجب في قانون مكافحة جرائم تقنية المعلومات على مقدم الخدمة المحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم افشائها أو الافصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة – ويشمل ذلك البيانات الشخصية لأى من مستخدمي خدمته أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصلون معها، كما أوجب عليه أيضاً ضرورة القيام بتأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اعتراضها أو اختراقها أو تلفها [137].

ومن أجل ذلك نهيب بالمشرع المصري والمنظم السعودي أن يتدخلا بالنص صراحة على تجريم سرقة الهوية من شبكة المعلومات أو مواقع التواصل الاجتماعي، وسندنا في ذلك أن جريمة انتحال الصفة تختلف في مضمونها عن سرقة هوية شخص من شبكة الإنترنت، فالأولى تتحقق بالتداخل في الوظيفة بأعمال إيجابية، بينما سرقة الهوية تتم من خلال أخذ المعلومات الشخصية الخاصة بشخص آخر دون علمه، ويلجأ القرصان (الهاكر) إلى ذلك بهدف الحصول على بطاقة ائتمان باسم ذلك الشخص أو عنوانه لفتح حساب مصرفي جديد، أو إنشاء (الشيكات) المزورة باستخدام الاسم، ورقم الحساب البنكي ، والحصول على شيكات، ومن هنا تتضح لنا جلياً أوجه الاختلاف الكبير بين سرقة الهوية وانتحال الصفة والبيانات،

135. د. خالد حامد مصطفي ، المسؤولية الجنائية لناشر الخدمات التقنية ومقدميها عن سوء استخدام شبكات التوصل الاجتماعي ، مجلة رؤي استراتيجية ، مركز الامارات للدراسات والبحوث الاستراتيجية ، المجلد الاول ، العدد 3 ، مارس ، 2013 ، ص 11

136. د. عمرو عيسي الفقي ، الجرائم المعلوماتية – جرائم الحاسب الالي والانترنت فيمصر والدول العربية ، المكتب الجامعي الحديث، الاسكندرية ، 2006م ، ص 102 . صغير يوسف ، الجريمة المرتكبة عبر الانترنت ، أطروحة ماجستير ، كلية الحقوق والعلوم السياسية ، جامعة مولود معمري ، تيزي وزو ، 2013 م ، ص 51.

137. حيث تنص المادة 2/أولاً/2–3 من قانون مكافحة جرائم تقنية المعلومات المصري.

وتُعد أهمية تجريم سرقة الهوية بنص صريح أمراً واضحاً وجلياً؛ لأن من شأنه أن يحمي البيانات الشخصية للمستخدم على مواقع التواصل الاجتماعي، ويحول دون استغلال هذه البيانات في ارتكاب جرائم أخرى.

ثانيا: جرائم التحايل على المواقع الالكترونية ومواقع التواصل الاجتماعي.

فجرائم التحايل على المواقع واختراقها والاستيلاء عليها تعد سبباً من أسباب ازدياد جرائم سرقة الهوية ثم استغلالها في ارتكاب جرائم احتيال ، أو تشهير وقذف، وتفيد التقارير بأن 3.5 مليون مستخدم تكبدوا خسائر تقدر بـ 3.2 مليار دولار بسبب هذه الإعلانات عبر البريد الإلكتروني غير المرغوب فيه باستغلال بوابة البنوك، وهذه المعلومات يسيء استخدامها المحتالون على شبكة الإنترنت من خلال سرقة بطاقات الائتمان وسحب أموال أصحابها من البنوك، أو اصطياد الضحايا عبر الإنترنت من خلال إجراء مزاد وهمي أو عرض تأشيرات وهمية مزورة وقد يستغل الفيسبوك Facebook في التعرف إلى بيانات الأشخاص من خلال معلوماتهم وجهات الاتصال الخاصة بهم ، وعناوين البريد الإلكتروني ، ثم يتم إرسال العديد من رسائل البريد المزعج إليهم وبسبب الخسائر الناجمة عن هذه الأفعال [138].

ثالثاً: جرائم استغلال العيوب التقنية واختراق المواقع الالكترونية ومواقع التواصل الاجتماعي.

وتتم عن طريق القراصنة مخترقي الانظمة علي مواقع التواصل الاجتماعي ، حيث يتبادل أفراد هذه الطائفة المعلومات فيما بينهم بغية الاطلاع علي مواطن الضعف في الانظمة المعلوماتية ، وتجري عملية التبادل للمعلومات بينهم بواسطة النشرات الاعلامية الالكترونية ، بل انهم يعقدون المؤتمرات لكافة مخترقي الانظمة المعلوماتية للتشاور حول وسائل الاختراق واليات نجاحها ،وكيفية استغلال العيوب التقنية علي الانترنت وشبكات التواصل ، ويتبع المخترقون أساليب عدة في عمليات تشويه صفحا المواقع وتختلف هذه الاساليب من موقع لأخر حسب نوع نظام التشغيل الذي يعتمد عليه الموقع [139].

حيث تستغل العيوب التقنية والثغرات الامنية في مزودات الويب وانظمة التشغيل ، فلا يخلوا أي نظام تشغيل او مزود ويب من ثغرات امنية تعرض مستخدميه للاختراق ، حيث يشتغل المخترقون الثغرات الامنية في عمليات الاختراق علي ان تجد الشركة المصممة للنظام الحل المناسب لها ، وتبقي بعض الثغرات والعيوب الفنية متاحة لفترة طويلة حتي يتم اكتشافها ، وذلك لان اغلب الثغرات التي يكتشفها

138. د. خالد حامد مصطفي ، المسؤولية الجنائية لناشر الخدمات التقنية ومقدميها عن سوء استخدام شبكات التوصل الاجتماعي ، مرجع سابق ، ص 12 .

139. صغير يوسف ، الجريمة المرتكبة عبر الانترنت ، المرجع السابق ، ص 31 و 32 .

المخترقون لا يعلنون عنها بسرعة ليتمكنوا من استغلالها لفترة اطوال [140].

المبحث الثاني

دور مواقع التواصل الاجتماعي والمواقع الالكترونية في عملية جمع الاستدلالات

نتيجة لما تتميز به شبكات التواصل الاجتماعي والمواقع الالكترونية من سهولة الحصول على المعلومات، كونها تُعد حقلا خصباً للسلطات في الحصول على المعلومات، فمن هنا يثار تساؤل مهم عن مدى إمكانية استخدام هذه الشبكات في جمع الاستدلالات عن جرائم المعلومات، حيث نرى إمكانية استخدام هذه المواقع في جمع الاستدلالات عن جرائم المعلومات، حيث يعتمد ضبط الجريمة واثباتها في المقام الاول علي جمع الادلة التي حدد المشرع وسائل اثباتها وجمع الاستدلال، حيث تتجسد أول طرق مكافحة الجرائم المرتكبة عبر الانترنت ووسائل التواصل الاجتماعي في الاستدلال الذي يتضمن كل من التفتيش والمعاين والخبرة، والتي تثير اشكالات اجرائية تعود الي خصوصية الجريمة المرتكبة عبر الانترنت ووسائل التواصل الاجتماعي، أما غيرها كالاستجواب وسماع الشهود فإننا نستبعدها نظراً لعدم وجود أي صعوبات في اتخاذها.

كما تُعد مواقع التواصل الاجتماعي أداة ممتازة لجمع المعلومات؛ لأنها تتضمن معلومات مهمة عن المستخدمين، وبالتالي يمكن للشرطة استخدامها في جمع الاستدلالات عن جرائم المعلومات، فهي توفر الجهد والوقت والمال في جمع المعلومات، فمن خلالها يمكن التوصل إلى معلومات عن الهويتين الحقيقية والافتراضية، فضلاً عن كونها تمثل هذه الشبكات فرصة حقيقية للسلطات في الوصول إلى البيانات، كما يمكن استخدامها في التحقيقات الأكثر حساسية. فعلى سبيل المثال، تُستخدم في فرنسا الشبكات الاجتماعية لجمع المعلومات في جرائم الخطف، والتحريض على الانتحار أو الكراهية العنصرية، والتشهير، والاتجار في المواد المخدرة، وجرائم الاعتداء الجنسي على الأطفال [141].

وبناء على ما سبق يمكن استخدام هذه المواقع والصفحات الشخصية في إجراءات جمع الاستدلالات عن الجرائم بمعرفة الشرطة المتخصصة، فمن خلال تحليل شبكات الفيسبوك يمكن تحديد العلاقات بين المشتبه فيهم والجرائم الناشئة عن الشبكات الاجتماعية.

وإذا كانت مواقع التواصل الاجتماعي توفر للسلطات معلومات مهمة عن مستخدمي هذه المواقع، فإنه ينبغي عند استخدام هذه المواقع في جمع الاستدلالات مراعاة التوازن بين مصلحة الشخص في الحفاظ على سرية المعلومات والحق في الخصوصية من ناحية، ومصلحة العدالة الجنائية في الوصول إلى

---

140. د. عمر بن محمد العتيني ، الامن المعلوماتي في المواقع الالكترونية ومدي توافقه مع المعايير المحلية والدولية ، أطروحة دكتوراه ، جامعة نايف العربية للعلوم الامنية ، كلية الدارسات العليا ، الرياض ، 2010 م ، ص 49 و 50 .

141. د. خالد حامد مصطفي ، المسؤولية الجنائية لناشر الخدمات التقنية ومقدميها عن سوء استخدام شبكات التوصل الاجتماعي ، مرجع سابق ، ص 23 .

المعلومات التي تسهم في كشف الحقيقة عن الجرائم المعلوماتية من ناحية أخرى، ومن هنا ينبغي الاعتراف بالدليل المستمد من المعلومات التي تم الحصول عليها من شبكات التواصل الاجتماعي، فهناك من يرى أن البيانات المخزنة الياً لا تصلح لأن تكون محلا للضبط بالكيفية المنصوص عليها في القوانين الإجرائية التقليدية بسبب انتفاء الطابع المادي عن هذه البيانات[142].

وهناك من يرى إمكانية استخدام المعلومات الواردة على الشبكات الاجتماعية، ولا يحول دون ذلك الطبيعة اللامادية ؛ فقد تكون هذه البيانات مسجلة على الصفحات الشخصية أو ثابتة في صندوق البريد الخاص بالمجني عليه، صادرة عن البريد الإلكتروني للجاني، وعندئذ يجوز نسخ هذه البيانات واسترجاعها وعرضها ، فإذا تبين أنها تشمل جريمة جاز استخدام الدليل الناشئ عن ذلك في الإدانة ، فالمشكلة لا تكمن في طبيعة البيانات بقدر ما تتعلق بضرورة تأهيل القائمين على الضبط، والتزام تقنيات فنية في ضبط هذه الأدلة [143]، مع مراعاة الشروط التي تجعل من ذلك الدليل مشروعاً؛ فعدم مشروعية الدليل من شأنه أن يهدر قيمته في الإثبات، ومن ثم لا يعول عليه كدليل في الإدانة [144].

المبحث الثالث

موقف المشرع المصري والسعودي تجاه جرائم التواصل الاجتماعي

تعاظمت مخاطر الجريمة في العصر الحديث وتحديداً منذ حدوث الثورة التكنولوجية وما نجم عنها من إفرازات سلبية أدت إلى ظهور نوعٍ جديدٍ غير مألوف من الجرائم ألا وهو "الجرائم الإلكترونية" والتي تعدّ أشد خطراً وأعظم ضرراً من العديد من أنماط الجرائم التقليدية لا سيما في المستوى المهارى والفني لمرتكبيها في مجال استخدام التكنولوجيا أو أدوات ارتكابها أو الحيز المكاني والزماني لها، وكونها تعدّ من الجرائم العابرة للوطنية في الكثير من أنماطها وهو ما يضعف من قدرات وإمكانات وأساليب مواجهتها في حالات عدة [145].

---

142. د. هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية ، مكتبة الآلات الحديثة ، أسيوط ، 1994 م ، ص 194.

143. د. عبدالفتاح بيومي حجازي ، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية ، دار النهضة العربية ، القاهرة ، الطبعة الاولي ، 2009 ، ص 276.

144. د. رؤوف عبيد ، مبادئ الإجراءات الجنائية في القانون المصري ، دار الفكر العربي ، القاهرة ، 1972 م ، ص 678 وما بعدها .

145. مستشار محمد أحمد محمد الحمادي ، تشريعات مكافحة جرائم تقنية المعلومات في دولة الإمارات وأحكام القضاء ، دولة الإمارات العربية المتحدة ، أبوظبي ، شرطة أبوظبي ، مركز الدراسات الأمنية ، ورقة عمل قدمت بندوة شبكات الإنترنت وتأثيراتها الاجتماعية والأمنية ، الطبعة الثانية ، الفترة من 6/7 نوفمبر 2006 م ، ص 9 .

ولقد واجه المشرع المصري جرائم الالكترونية ومن ضمنها جرائم التي تقع علي مواقع التواصل الاجتماعي ، حيث تصدي لها وجرمها وفق الآتي:

أولا: جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات:

1. جرائم الانتفاع دون وجه حق بخدمات تقنية المعلومات:

بغرض تقنين مسائل الانتفاع بخدمات تقنية المعلومات ومنها مواقع التواصل الاجتماعي بحيث لا ينتفع بها إلا من كان له وجه حق في ذلك، نجد أن المشرع المصري في قانون مكافحة جرائم تقية المعلومات قد جرم فعل كل من انتفع بدون وجه حق عن طريق شبكة النظام المعلوماتي، أو إحدى وسائل تقنية المعلومات، بخدمة من خدمات اتصالات أو خدمات قنوات البث المسموع والمرئي، وعاقبه بالحبس مدة لا تقل عن 3 شهور وبغرامة لا تقل عن 10 ألف جنيه ولا تجاوز 50 ألف جنيه أو بإحدى هاتين العقوبتين [(146)].

2. جريمة تجاوز حدود الحق في الدخول:

كما جرم المشرع المصري في قانون مكافحة جرائم تقية المعلومات كافة الجرائم التي يتجاوز من خلالها الشخص حدود الحق في الدخول، حيث عاقب المشرع المصري مرتكب تلك الجريمة بالحبس مدة لا تقل عن 6 أشهر وبغرامة لا تقل عن 30 ألف جنيه ولا تجاوز 50 ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدما حقا مخولا له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول [(147)].

3. جريمة الدخول غير المشروع للمواقع أو اعتراضها:

ويتمثل القصد الجنائي لهذه الجريمة في ركنين اثنين هما الدخول غير المشروع للموقع وقصد الحصول على المعلومات، ولا عبرة هنا باتجاه نية الجاني لتحقيق أثر محدد، يستوي في هذه الحالة توجه الإرادة إلي إحداث الاتلاف من عدمه، حيث فرق المشرع المصري في العقاب بين مجرد الدخول غير المشروع سواء اكان هذا الدخول عمداً أو عن طريق الخطأ، وبين الدخول غير المشروع بقصد إحداث إتلاف أو محو او تغيير أو نسخ أو إعادة نشر للبيانات والمعلومات على ذلك الموقع.

كما جرم المشرع المصري في قانون مكافحة جرائم تقية المعلومات كافة الجرائم التي يتم الدخول فيها للمواقع الالكترونية بصورة غير مشروعة، حيث عاقب المشرع المصري مرتكب تلك الجريمة يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن 50 ألفا ولا تجاوز 100 ألف جنيه، أو إحدى هاتين العقوبتين، كل من دخل عمدا أو دخل بخطأ غير عمدى وبقى بدون وجه حق، على موقع أو حساب خاص

---

146. راجع نص المادة 13 من قانون مكافحة جرائم تقنية المعلومات المصري.

147. راجع نص المادة 14 من قانون مكافحة جرائم تقنية المعلومات المصري.

أو نظام معلوماتي محظور الدخول عليه، أما إذا أنتج عن ذلك الدخول الغير مشروع حدوث إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، تكون العقوبة الحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 100 ألف جنيه ولا تجاوز 200 ألف أو بإحدى هاتين العقوبتين [148].

كذلك الحال جرم المشرع المصري كافة أشكال الاعتراض التي تتم في مواجهة المعلومات والبيانات وكل ما هو متداول عبر مواقع التواصل الاجتماعي وكافة الموقع الالكترونية ، حيث عاقب المشرع المصري جريمة اعتراض المعلومات والبيانات وكل ما هو متداول عبر مواقع التواصل الاجتماعي وكافة الموقع الالكترونية بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 250 ألف جنيه، أو بإحدى هاتين العقوبتين كل من اعترض بدون وجه حق أية معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الألى وما في حكمها **(المادة 16 مصري)**.

وفي النظام السعودي نجد أنه جرم فعل الدخول غير المشروع للمواقع الالكترونية، حيث عاقب بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب فعل الدخول عير المشروع لتهديد شخص أو ابتزازه، وذلك لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً، أو إذا كان الدخول إلي الموقع الالكتروني بغرض تغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه [149].

4. جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية:

وهي جريمة تتعلق بالتلاع في المعلومات داخل مواقع التواصل الاجتماعي كذا مختلف النظم المعلوماتية بغرض تغيير الحقيقة فيها، وهذا التلاعب قد يتم عن طريق تعديل هذه المعلومات أو من خلال محو جزاء أو عدة اجزاء منها، فعملية تعديل المعلومات والمعطيات تقنية سهلة وشائعة من تقنيات الإجرام المعلوماتي[150].

كما جرم المشرع المصري كافة جرائم الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية، حيث عاقب كل من أتلف أو عطل أو عدل مسار أو ألغى كلياً أو جزئياً، متعمداً وبدون وجه حق، البرامج والبيانات أو المعلومات المخزنة، أو المعالجة، أو المولدة أو المخلقة على أي نظام معلوماتي وما في

148. راجع نص المادة 15 من قانون مكافحة جرائم تقنية المعلومات المصري.

149. راجع نص المادة 3/2-3 من النظام السعودي.

150. راجع نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 1429ه/ 2008م ، ص 148.

حكمه، أيا كانت الوسيلة التي استخدمت في الجريمة بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن100 ألف جنيه ولا تجاوز 500 ألف جنيه، أو بإحدى هاتين العقوبتين [151].

وفي النظام السعودي نجد أنه جرم فعل الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها، أو تغييرها، أو إعادة نشرها، ففي كل تلك الجرائم تكون العقوبة السجن مدة لا تزيد على أربع سنوات، وبغرامة لا تزيد على ثلاثمائة ملايين ريال، أو بإحدى هاتين العقوبتين [152].

5. جريمة الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة:

يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 100 ألف جنيه أو بإحدى العقوبتين كل من أتلف أو عطل أو أبطأ أو اخترق بريدا إلكترونيا أو موقعا أو حسابا خاصا بأحد الناس. فإذا وقعت الجريمة على بريد إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة الحبس مدة لا تقل عن 6 أشهر وبغرامة لا تقل عن 100 ألف جنيه ولا تجاوز 200 ألف جنيه أو بإحدى هاتين العقوبتين [153].

جريمة الاعتداء على تصميم موقع:

يعاقب بالحبس مدة لا تقل عن 3 أشهر، وبغرامة لا تقل عن 20 ألف جنيه ولا تجاوز 100 ألف جنيه أو بإحدى العقوبتين، كل من أتلف أو عطل أو أبطأ أو شوه أو اخفى، أو غير تصاميم موقعاً خاصاً بشركة أو مؤسسة أو منشأة أو شخص طبيعي بغير وجه حق [154].

6. جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة:

حيث استغلت الكثير من الجماعات المتطرفة الطبيعة الاتصالية للإنترنت من اجل بث معتقداتها وأفكارها، بل تعداه الأمر إلي ممارسات تهدد أمن الدولة المعتدى عليها، خاصة المتمثلة في الارهاب والجريمة المنظمة، اللذان أخذا منحى آخر في استعمال الانترنت ووسائل التواصل الاجتماعي، التي سمحت لهم في ارتكاب جرائم غاية في الفتك في حق المجتمعات والدول، بل الأخطر من ذلك أنها أتاحت للكثير

151. راجع نص المادة 17 من قانون مكافحة جرائم تقنية المعلومات المصري.

152. راجع نص المادة 1/5 من النظام السعودي.

153. راجع نص المادة 18 من قانون مكافحة جرائم تقنية المعلومات المصري.

154. راجع نص المادة 19 من قانون مكافحة جرائم تقنية المعلومات المصري.

من الدول ممارسة التجسس علي دول أخري وذلك بالاطلاع علي مختلف الأسرار العسكرية والاقتصادية لهذه الاخيرة [155].

لذا عاقب المشرع المصري كل من دخل عمدا أو بخطأ غير عمدى وبقى بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعا أو بريدا إلكترونيا أو حسابا خاصا أو نظاما معلوماتيا يدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوك لها أو يخصها بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 200 ألف جنيه، أو بإحدى هاتين العقوبتين، إما إذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية تكون العقوبة السجن والغرامة التي لا تقل عن 100 ألف جنيه ولا تجاوز 500 ألف جنيه، وفى جميع الأحوال، إذا ترتب على أي من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي أو البريد الإلكتروني أو تدميرها أو تشويهها أو تغييرها أو تغييرها أو تصميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها أو إلغائها كليا أو جزئيا بأي وسيلة كانت، تكون العقوبة السجن والغرامة التي لا تقل عن مليون جنيه ولا تجاوز 5 ملايين جنيه [156].

كما جرم المنظم السعودي كل فعل من شأنه أن يؤدي إلي الدخول غير المشروع إلي موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني، ففي كل تلك الجرائم تكون العقوبة السجن مدة لا تزيد على عشر سنوات، وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين [157].

7. جريمة الاعتداء على سلامة الشبكة المعلوماتية:

يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه أو بإحدى هاتين العقوبتين، كل من تسبب متعمدا في إيقاف شبكة معلوماتية عن العمل أو تعطيلها، أو الحد من كفاءة عملها، أو التشويش عليها، أو إعاقتها، أو اعتراض عملها، أو أجرى بدون وجه حق معالجة الكترونية للبيانات الخاصة بها. ويعاقب كل من تسبب بخطأه في ذلك، بالحبس مدة لا تقل عن ثلاث شهور، وبغرامة لا تقل عن خمسون ألف جنيه ولا تجاوز مائتي ألف جنيه أو بإحدى العقوبتين،

155. عبد الله بن عبد العزيز االيوسفي ، أساليب تطور البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة ، جامعة نايف العربية للعلوم الامنية ، الرياض ، الطبعة الاولي ، 2004 م ، ص 25 .

156. راجع نص المادة 20 من قانون مكافحة جرائم تقنية المعلومات المصري.

157. راجع نص المادة 2/7 من النظام السعودي.

فإذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة، أو تدار بمعرفتها أو تمتلكها، تكون العقوبة السجن المشدد وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه [158].

وفي النظام السعودي نجد أن المنظم السعودي كذلك جرم كل فعل من شأنه أن يؤدي إلي إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدميرها، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها، أو إعاقة الوصول إلي الخدمة، أو تشويشها، أو تعطيلها بأي وسيلة كانت، ففي كل تلك الجرائم تكون العقوبة السجن مدة لا تزيد على أربع سنوات، وبغرامة لا تزيد على ثلاثمائة ملايين ريال، أو بإحدى هاتين العقوبتين [159].

ثانياً: الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات:

1. جرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني.

يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر والغرامة التي لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، في الوصول بدون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الالكترونية فإن قصد من ذلك استخدامها في الحصول على أموال الغير أو ما تتيحه من خدمات، يعاقب بالحبس مدة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين. وتكون العقوبة الحبس مدة لا تقل عن سنة، والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز 200 ألف، أو إحدى هاتين العقوبتين، إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير [160].

وفي النظام السعودي نجد أن نظام مكافحة جرائم المعلوماتية جرم كل فعل من شأنه الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة، وكذا كل فعل من شأنه الوصول دون مسوغ نظامي صحيح إلي بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو

158. راجع نص المادة 21 من قانون مكافحة جرائم تقنية المعلومات المصري.

159. راجع نص المادة 2/5-3 من النظام السعودي.

160. راجع نص المادة 23 من قانون مكافحة جرائم تقنية المعلومات المصري.

أموال، أو ما تتيحه من خدمات، فعاقب المنظم السعودي عن كل تلك الأفعال بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين [161].

2. الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني بغرض الاتجار بالبشر أو المواد الاباحية أو المخدرات.

يعاقب بالحبس مدة لا تقل عن 3 أشهر وغرامة لا تقل عن 10 آلاف جنيه ولا تجاوز 30 ألف جنيه أو بإحدى العقوبتين كل من اصطنع بريدا إلكترونيا أو موقعاً أو حاساباً خاصاً ونسبه زوراً لشخص طبيعي أو اعتباري. فإذا استخدم الجاني البريد أو الموقع أو الحساب الخاص المصطنع في أمر يسئ إلى من نسب إليه، تكون العقوبة الحبس الذى لا تقل مدته عن سنة وغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 200 ألف جنيه أو بإحدى العقوبتين. وإذا وقعت الجريمة على أحد الأشخاص الاعتبارية العامة فتكون العقوبة السجن والغرامة التي لا تقل عن 100 ألف جنيه ولا تزيد على 300 ألف جنيه **(المادة 24 مصري).**

وفي النظام السعودي نجد أن نظام مكافحة جرائم المعلوماتية جرم كل فعل من شأنه إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي، وكذا جرم كل فعل من شأنه إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره بغرض الاتجار في الجنس البشري، أو تسهيل التعامل به، أو إنشاء مواد أو بيانات متعلقة بالمواقع الاباحية، أو الأنشطة المتعلقة بالميسر والمخلفة بالآداب العامة وكذا العمل على نشرها أو ترويجها، أو إنشاء مواقع بغض الاتجار بالمخدرات والمؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل معها، فعاقب المنظم السعودي عن كل تلك الأفعال بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين [162].

3. جرائم التهديد المعلوماتي للحياة الخاصة.

تعد الحياة الخاصة قطعة غالية من كيان الإنسان لا يمكن انتزاعها منه، وإلا تحول في هذه الحالة إلي اداء صماء خالية من القدرة على الإبداع الإنساني، فالإنسان بحكم طبيعته له أسراره الشخصية ومشاعره الذاتية وصلاته الخاصة وخصائصه المتميزة ولا يمكن له أن يتمتع بها إلا في دائرة مغلقة يحفظها ويهيأ لها سبل البقاء، كما تقتضي حرمة هذه الحياة أن يكون للإنسان الحق في إفضاء السرية على مظاهرها، وفي

161. راجع نص المادة 4 من النظام السعودي.

162. راجع نص المادة 6 من النظام السعودي.

إطار المعلوماتية تبرز خطورة التهديد المعلومات للحياة الخاصة بشكل أساسي في إساءة استخدام المعلومات والبيانات المتعلقة بالأفراد [163].

وفي سبيل إضفاء المزيد من الحماية على الحياة الخاصة لأفراد من وقوعها فريسة لاستباحة مواقع التواصل الاجتماعي وكذا المواقع الالكترونية لها عاقب المشرع المصري في قانون مكافحة جرائم تقنية المعلومات المصري كل من اعتدى على أي من المبادئ أو القيم الاسرية في المجتمع المصري، أو انتهك حرمة الحياه الخاصة أو ارسل بكثافة العديد من الرسائل الاليكترونية لشخص معين دون موافقته، أو منح بيانات إلى نظام أو موقع اليكترونى لترويج السلع أو الخدمات دون موافقته أو بالقيام بالنشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، لمعلومات أو اخبار أو صور وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة ام غير صحيحة بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين [164].

بل جرم المشرع المصري كافة ربط البيانات الشخصية للأفراد بأي محتوي مناف للآداب العامة، فعاقب كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى مناف للآداب العامة أو لإظهارها بطريقة من شانها المساس باعتباره أو شرفه بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات وبغرامة لا تقل عن مائة ألف جنيه لا تجاوز 300 ألف جنيه أو بإحدى [165].

وفي النظام السعودي عاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين كل فعل يرتكب بغرض التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد اجهزة الحاسب الآلي دون وجه حق أو التقاطه أو اعتراضه، أو المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا أو ما في حكمها، أو التشهير بالآخرين، وإلحاق الضرر بهم عبر وسائل تقنية المعلومات المختلفة [166].

ثالثاً: الجرائم المرتكبة من مدير الموقع:

في غير الأحوال المنصوص عليها في هذا القانون، يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 100 ألف جنيه ولا تزيد عن 300 ألف جنيه أو بإحدى هاتين العقوبتين، كل من أنشا أو أدار

163. راجع نهلا عبد القادر المومني، الجرائم المعلوماتية، مرجع سابق ، ص 172.

164. راجع نص المادة 25 من قانون مكافحة جرائم تقنية المعلومات المصري.

165. راجع نص المادة 26 من قانون مكافحة جرائم تقنية المعلومات المصري.

166. راجع نص المادة 3/1-4-5 من النظام السعودي.

أو استخدم موقعا أو حسابا خاصا على شبكة معلوماتية يهدف إلى ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانوناً [167].

كما يعاقب بالحبس مدة لا تقل عن 6 أشهر وبغرامة لا تقل عن 20 ألف ولا تجاوز 200 ألف أو إحداي هاتين العقوبتين، كل مسئول عن إدارة موقع أو حساب خاص أو بريد إلكتروني أو نظام معلوماتي، إذا أخفى أو عبث بالأدلة الرقمية لإحدى الجرائم المنصوص عليها في هذا القانون والتي وقعت على موقع أو حساب أو بريد إلكتروني بقصد إعاقة عمل الجهات الرسمية المختصة [168].

يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن 20 ألف ولا تجاوز 200 ألف جنية، أو بإحدى هاتين العقوبتين كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإليكتروني أو النظام المعلوماتي عرض أي منهم لإحدى الجرائم المنصوص عليها في هذا القانون.ويعاقب بالحبس مدة لا تقل عن 6 أشهر وبغرامة لا تقل عن 10 الاف جنية ولا تجاوز 100 ألف جنية أو بإحدى هاتين العقوبتين كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإليكتروني أو النظام المعلوماتي، تسبب بإهماله في تعرض أي منهم لإحدى الجرائم المنصوص عليها في هذا القانون، وكان ذلك بعدم اتخاذه التدابير والاحتياطات التأمينية الواردة في اللائحة التنفيذية [169].

غير أن المنظم السـعودي لم يتطرق ي نظام مكافحة جرائم المعلوماتية إلي تجريم الجرائم الواقعة بواسطة مدير المواقع، وربما يقصد بعدم تخصيص مدير المواقع بعقوبات معينة إيقاع ذات العقوبات الواردة بالنظام على الجميع، وإن كانا نهيب بالنظم السـعودي الن على عقوبات مشـددة توقع على مدير الموقع نظراً لمسؤوليته الخطيرة والصلاحيات التي توجد تحت يده.

الخاتمة .

بعد الانتها من هذا البحث والذي تناولنا فيه الحديث عن جرائم التواصل الاجتماعي، حيث تبين لدي مدي خطورة هذه المواقع في استخدامها لارتكاب مجموعة من الجرائم، حيث تناولنا الحديث في التمهيد عن بيان ماهية شبكات التواصل الاجتماعي والجرائم المعلوماتية، بينما نتناول في المبحث الاول بيان أهم الجرائم المرتكبة عبر المواقع الإلكترونية، وفي المبحث الثاني ألقينا الضوء على دور المواقع الالكترونية في عملية جمع الاستدلالات، واخيراً تناولنا في المبحث الثالث بيان موقف كلاً من المشرع المصري والمنظم السعودي تجاه جرائم تقنية المعلومات.

وخلصنا الي مجموعة من النتائج والتوصيات أهمها الاتي:

النتائج .

167. راجع نص المادة 27 من قانون مكافحة جرائم تقنية المعلومات المصري.

168. راجع نص المادة 28 من قانون مكافحة جرائم تقنية المعلومات المصري.

169. راجع نص المادة 29 من قانون مكافحة جرائم تقنية المعلومات المصري.

1. تعد مواقع التواصل الاجتماعية وسيلة الكترونية حديثة للتواصل الاجتماعي بين الأفراد بكل سهولة ويسر.
2. يُقصد بسرقة الهوية الحصول بوسائل احتيالية على معلومات من الإنترنت تخص شخصاً معيناً، مثل الاسم، وتاريخ الميلاد، والمهنة، والجنسية وكافة بيانات تتعلق بهويته وشخصية وذلك دون علمه.
3. لم يضع المشرع المصري نصاً صريحاً يُجرم سرقة الهوية، وبالتالي لا تُعد جريمة سرقة الهوية في حد ذاتها جريمة، إلا إذا استتبعها انتحال الشخصية، أو استبدالها في محرر أُعد لإثباتها.
4. جرائم استغلال العيوب التقنية تتم عن طريق القراصنة مخترقي الانظمة علي مواقع التواصل الاجتماعي.
5. تتجسد أول طرق مكافحة الجرائم المرتكبة عبر الانترنت ووسائل التواصل الاجتماعي في الاستدلال الذي يتضمن كل من التفتيش والمعاين والخبرة.
6. تُعد مواقع التواصل الاجتماعي أداة ممتازة لجمع المعلومات؛ لأنها تتضمن معلومات مهمة عن المستخدمين وبالتالي يمكن للشرطة استخدامها في جمع الاستدلالات عن جرائم المعلومات.
7. ينبغي عند استخدام مواقع التواصل الاجتماعي في جمع الاستدلالات مراعاة التوازن بين مصلحة الشخص في الحفاظ على سرية المعلومات والحق في الخصوصية من ناحية، ومصلحة العدالة الجنائية في الوصول إلى المعلومات التي تسهم في كشف الحقيقة عن الجرائم المعلوماتية من ناحية أخرى.

التوصيات.

1. نهيب بالمشرع المصري والسعودي ضرورة القيام بتدريب كافه أجهزة الشرطة على الأنظمة المعلوماتية، وقواعد البيانات، وكيفية استخدام أدوات الحاسب، حتى يكونوا على أتم استعداد لمواجهه تلك الجرائم.
2. ضرورة انشاء جهات متخصصة ومتفرغة لمكافحة كافة الجرائم الواقعة عبر مواقع التواصل الاجتماعي، بحث تكون على مستوي عالٍ من الخبرات التقنية.
3. ضرورة نشر الوعي الثقافي لدى الآباء والمجتمع لخطورة مواقع التواصل الاجتماعي، ولما قد يحدث من جرائم من خلالها.
4. نهيب بالمنظم السعودي النص على عقوبات خاصة لمدير الموقع وعدم الاكتفاء بتلك العقوبات التي توقع على الجميع.

قائمة المراجع:

أولا: المراجع العامة والمتخصصة:

1. خالد ممدوح ابراهيم، امن الجريمة الالكترونية، الدار الجامعية، الاسكندرية، 2010م.
2. رؤوف عبيـــــــد ، مبادئ الإجراءات الجنائية في القانون المصري، دار الفكر العربي، القاهرة، 1972 م.
3. عبد الله بن عبد العزيز االيوســـفي، أســـاليب تطور البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة، جامعة نايف العربية للعلوم الامنية، الرياض، الطبعة الاولي، 2004 م.
4. عبدالفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دار النهضة العربية، القاهرة، الطبعة الاولي ، 2009.
5. عبدالله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، الطبعة الثانية، 2002 م.
6. عمرو عيسي الفقي، الجرائم المعلوماتية – جرائم الحاسب الالي والانترنت فيمصر والدول العربية، المكتب الجامعي الحديث، الاسكندرية، 2006م.
7. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشـــر والتوزيع، عمان، الأردن، 1429هـ/ 2008م.
8. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوطـــــ، مصر ، 1994 م.

ثانيا: الدوريات والرسائل العلمية.

1. خالد حامد مصطفي، المسؤولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الاجتماعي، مجلة رؤي استراتيجية، مركز الامارات للدراسات والبحوث الاستراتيجية، المجلد الاول، العدد 2، مارس 2013 م.
2. رانيا عبد الله الشريف، دور وسائل التواصل الاجتماعي في انتشار الشائعات، بحث مقدم لمجلة العلاقات العامة والإعلان، الجمعية السعودية للعلاقات العامة والإعلان، السعودية، العدد 3، 2015م.
3. صـــغير يوســـف ، الجريمة المرتكبة عبر الانترنت، أطروحة ماجســـتير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013 م.

4. عمر بن محمد العتيبي، الامن المعلوماتي في المواقع الالكترونية ومدي توافقه مع المعايير المحلية والدولية، أطروحة دكتوراه، جامعة نايف العربية للعلوم الامنية، كلية الدراسات العليا، الرياض، 2010 م.

5. محمد أحمد محمد الحمادي، تشريعات مكافحة جرائم تقنية المعلومات في دولة الإمارات وأحكام القضاء، دولة الإمارات العربية المتحدة ، أبوظبي، شرطة أبوظبي، مركز الدراسات الأمنية، ورقة عمل قدمت بندوة شبكات الإنترنت وتأثيراتها الاجتماعية والأمنية، الطبعة الثانية، الفترة من 6/7 نوفمبر 2006 م.

6. محمد محمد سيد احمد عامر، المسؤولية الجنائية عن ترويج الإشاعات عبر وسائل التواصل الاجتماعي دراسة فقهية مقارنة بالقانون المصري والنظام السعودي، بحث مقدم لمؤتمر وسائل التواصل الاجتماعي التطبيقات والإشكاليات المنهجية ، كلية الإعلام والاتصال، جامعة الإمام محمد بن سعود الإسلامية، الرياض، الفترة من19-1436/5/20هـ الموافق 10-2015/3/11م .

ثالثا: القوانين.

1. قانون مكافحة جرائم تقنية المعلومات المصري 175 لسنة 2018.
2. نظام مكافحة جرائم المعلوماتية 1428هـ، مرسوم ملكي رقم: م/17 بتاريخ 1428/3/8هـ.